



SYNCHRONIZE NETWORK DELIVERY

Warfighter Mission Area (WMA)

Net-Centric Data Strategy (NCDS)

"Data is a Key Enabler of Combat Power."



WMA Net-Centric Data Strategy (NCDS) implementation is two-pronged: WMA affiliated Community of Interest (COI) governance, and programs' Net-Ready Key Performance Parameter (NR-KPP) compliance. Governance of WMA-affiliated COIs is achieved through the WMA IT Domain Owners/Functional Capabilities Boards (FCB). Program compliance with the NCDS is enforced via interoperability and supportability (I&S) certifications.

A community of interest (COI) is a collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. COIs identify and address information sharing problems.

NCDS- and COI-related portions of CJCSI 8410.01, *Warfighting Mission Area Information Technology Portfolio Management and Data Sharing* (DRAFT) cover COI governance through the WMA IT Domains. This includes identification of information sharing problems, identifying candidate COIs to address them, and proposing DOD Components to lead the COIs. WMA-affiliated COIs will be governed by the appropriate WMA IT Domain Owner/FCB. Governance will include a structured mechanism for informing the Department's portfolio management processes relative to information sharing decisions. A draft COI Metrics Implementation Framework will provide a means to monitor COI progress.

Programs address compliance with the NCDS in Capability Development Documents (CDDs), Capability Production Documents (CPDs), and Information

Support Plans (ISPs).

This is enforced via I&S certifications described in CJCSI 6212.01D, *Interoperability and Supportability of Information Technology and National Security Systems*, 8 March 2006.

Specific NCDS compliance criteria are found in Enclosure D of CJCSI 6212.01D:

- Data shall be made visible, accessible, and understandable to any potential user in the Department of Defense.
- Data assets shall be made visible by creating and associating metadata ("tagging"), including discovery metadata, for each asset.
- Data assets shall be made accessible by making data available in shared spaces.
- Data assets shall be made understandable by publishing associated semantic and structural metadata in a federated DOD metadata registry.
- Data assets shall have associated information assurance and security metadata, and an authoritative source for the data shall be identified when appropriate.
- Data interoperability shall be supported by making data assets understandable and by enabling business and mission processes to be reused where possible.
- Semantic and structural agreements for data sharing shall be promoted through communities (e.g., communities of interest (COIs)), consisting of data users (producers and consumers) and system developers.

"Net-Centric Data Strategy compels a shift to a "many-to-many" exchange of data, enabling many users and applications to leverage the same data – extending beyond the previous focus on standardized, predefined point-to-point interfaces."

John P. Stenbit, Former DoD CIO, Department of Defense Data Strategy, May 9, 2003